Internet Privacy Concerns Revisited: Oversight from Surveillance and Right To Be Forgotten as New Dimensions

Gaurav Bansal [a,*] , Fiona Fui-Hoon Nah [b]

a University of Wisconsin – Green Bay, Green Bay, WI 54311, USA

b City University of Hong Kong, Hong Kong

Published in Information & Management (2022) 59, 103618. DOI: 10.1016/j.im.2022.103618

Abstract: In the post-Snowden revelation era, concerns related to government surveillance and oversight have come to the forefront. The ability of the Internet to remember "everything" (or forget anything) also raises a privacy concern associated with the right to be forgotten (RTBF). In this paper, we examine the conceptualization of Internet privacy concerns (IPC) by extending Hong and Thong's (2013) model with the addition of two dimensions: oversight (i.e., due to surveillance) and the RTBF. We provide theoretical and empirical evidence for our proposed integrated conceptualization. Data were collected from Amazon's Mechanical Turk and analyzed with structural equation modeling using a nomological network that includes trusting beliefs. This research contributes to a better understanding of the conceptualization of IPC and provides a reliable and valid contemporary instrument for IPC.

Keywords: Privacy concerns, Right to be forgotten, Surveillance, Oversight

1. Introduction

Privacy is a complex and dynamic concept [[37], [85]]. As data collection, storage, and retrieval increasingly become more pervasive, the concept of privacy will continue to evolve [26, 44, 48, 57, 86, 92]. The dimensions of Internet privacy concerns (IPC) will need to be reevaluated as concerns for information privacy evolve in the age of data collection and surveillance by not only the governments [76] but also corporations [104], including healthcare providers [42, 43], among others. The concerns are further aggravated given the reduction in control over the use of personal data [8] and the difficulty experienced by users to retract or minimize the consequences of releasing their personal information [48]. Today's technological advances, such as voice-enabled assistants [75], facial recognition [62], location-tracking phones and apps, and social media [69], to name a few, have fueled data collection, storage, extraction, transformation, and analytics. The proliferation of mobile apps [e.g., 42] and new AI-based applications such as autonomous driving [18] and robotic surgery [72] propel these concerns further. Data analytics have increased capabilities to generate insights on individual citizens by connecting the dots from people's identity, location, behavior, associations, and activities, while at the same time providing few, if any, safeguards to protect individuals from any wrongful or unethical use of their data.

In the post-9/11 world, governments collect more data to keep the borders safe, while businesses continue to increase their use of customer data for profiling and target marketing. People who historically were concerned about the collection, secondary use, and unauthorized access of data, as well as the inadequate protection of their data from errors, are now more concerned about other aspects of information privacy that were less salient in the pre-Snowden era [100], such as government surveillance and oversight [38] as well as the capability of the Internet to remember everything forever [7]. People are concerned about the constant surveillance and oversight/monitoring of their data taking place anytime and nearly everywhere, particularly with the Internet of things. We refer to this privacy concern as oversight from surveillance because of the constant surveillance and overseeing of individuals' activities. A recent survey by the Pew Research Center indicates that Americans' perspective of privacy concerns has changed, and 70% of Americans believe that the government is using surveillance data for purposes beyond anti-terror efforts [39]. Another survey by the Pew Research Center indicates that most Americans disapprove of the collection of citizens' data by the US government and that many of them have changed their behavior because of the government surveillance program [77]. Thus, the nature and concept of privacy concerns have undergone a silent change to warrant a closer examination. Although past research has conceptualized concerns for information privacy, these privacy concerns also need to be examined from the perspective of oversight or the possibility of constant surveillance, such as by the governments [38]. In the era following Snowden revelations, concerns related to government surveillance and oversight, directly or indirectly by corporate firms and businesses, have come to the forefront. Due to the typically low trust that Americans place in their governments and businesses [78], concerns associated with surveillance and oversight are a significant factor impacting privacy concerns.

The ability (or inability) of the Internet to remember "everything" (or forget anything) further fuels the concern that people are losing control of their personal information. Hence, the *right to be forgotten* (RTBF) is increasingly recognized as a concern of privacy [7, 89-91]. Several studies have argued for legalizing the RTBF in the USA because the US Constitution and laws accept some versions of the RTBF [e.g., 17, 58], whereas others have argued against it by indicating that the RTBF is at odds with the US Constitution's First Amendment [53]. However, surveys by the Pew Research Center have indicated that most Americans support the right to have some personal information removed from online searches. Most Americans would like to have the following information removed [7]: embarrassing photos and videos (87%), financial data prepared by tax preparers (79%), medical data collected by health care providers (69%), and data collected by law enforcement agencies (36%).

Against this backdrop, our research question is to explore a more complete conceptualization of IPC using oversight from surveillance and the *RTBF* as two additional dimensions. Drawing on the definitions of IPC in the literature [44, 57], we define IPC as the degree to which a person is concerned about Internet practices related to the collection and use of his or her personal information. To answer the research question, we draw on the multidimensional development theory (MDT) [41, 44, 54] that Hong and Thong [44] have utilized to examine the IPC model. MDT has been used to help understand individual perceptions of privacy. It purports that an individual's privacy concerns are jointly determined by factors pertaining to four key dimensions: individual, environmental, information management, and interaction management. MDT allows for considerations of dimensions that describe how individuals develop privacy concerns over time, where privacy concerns result from a self-development process that focuses on autonomy as well as the impact of changes in the environment. Hence, we will examine how the two new dimensions of IPC are classified based on MDT. Moreover, we examine the efficacy of the emerging IPC scale within the nomological network of trust constructs – trusting beliefs in the Internet, online businesses (in general), and government – to understand the extent to which predictions based on the newly enhanced IPC scale are assessed within a wider theoretical context or network [10, 86].

This paper also answers the call by Hong and Thong [44], who suggested that (1) the IPC dimensions are not static and could evolve over time, and hence, research is needed to revise and test the dimensionality of the IPC model to keep it relevant and up to date; (2) the lower-order dimensions of IPC will need to be reevaluated periodically, especially after significant social and technological changes that impact secondary usage or unauthorized monitoring of data, which may impact Internet users' privacy perceptions; and (3) the conceptualization of the IPC model will need to be tested in other countries where the social, cultural, societal, and technological environments could be different, as the model by Hong and Thong [44] was evaluated based on data from respondents in Hong Kong. Thus, we validate and extend the IPC model by Hong and Thong [44] in the context of two new dimensions that are of relevance and significance in the USA. We provide theoretical and empirical evidence for our proposed integrated conceptualization. This research thus contributes to a better understanding of the conceptualization of IPC and provides a reliable and valid contemporary instrument representing the state of IPC in the post-Snowden era.

The paper proceeds as follows: First, we present the related literature and theoretical development. Following that, we describe the field study and the data collected. Next, we present the data analysis and results. We then discuss the study's contributions and implications and conclude the paper.

2. Literature Review and Theoretical Development

Privacy refers to the right of individuals to determine for themselves when, how, and to what extent to release personal information to others [50, 99]. Specifically, we draw on Turn's definition of privacy as "the right of individuals regarding the collection, storage, processing, dissemination, and use of personal information about themselves" [98, p. 242].

The concept of information privacy concerns has undergone several changes since its conceptualization by Smith et al. [86] as comprising four dimensions: collection, secondary use, improper access, and error (see Hong and Thong [44], p. 280, for a summary). There have been several incremental modifications to the construct over the years. Stewart and Segars [92] proposed conceptualizing concerns for information privacy as a second-order construct with control as the binding force that ties the first-order factors of collection, secondary use, unauthorized access, and errors. Hong and Thong [44] conceptualized IPC as a third-order construct that comprises two second-order factors and one first-order factor, awareness. The two second-order factors are information management that comprises two first-order dimensions, improper/unauthorized access and error, and interaction management that comprises three first-order dimensions, namely, collection, secondary use, and control. Dinev and Hart [31], Earp et al. [34], and Xu et al. [106] also include monitoring as one of the dimensions. Steinbart et al. [90] examined the inclusion of the RTBF in their privacy concern model and indicated that the findings are inconclusive. We provide a brief overview of the evolution of salient privacy concern scales in Table 1, followed by definitions and comments on the various dimensions.

2.1. Definitions of Dimensions of Privacy Concerns

As shown in Table 1, we examine eight dimensions of privacy concerns from the literature. We discuss these dimensions next and summarize their definitions in Table 2.

Collection: This dimension has been used in all major privacy concern scales. The dimension is based on the principle of minimizing data collection to protect an individual's privacy [6]. It was inspired by Miller's [86] concern that "there's too much damn data collection going on in this society" [64].

Unauthorized/improper access: This dimension captures both technological capabilities and organizational policy in preventing unauthorized access to user data [86]; hence, it aims at understanding whether only the "right" individuals are allowed to access personal information in the files. It has been part of all major privacy concern scales except Malhotra et al. [57].

Secondary use (internal and external): This concern was mentioned in studies conducted in the 1970s, but it did not become a major concern of privacy until the 1980s [86]. This dimension is geared toward companies profiting from users' data by the sale or rental of their information [94]. It has been part of all major privacy concern scales except Malhotra et al. [57].

Errors: This dimension captures users' concern that organizations need to protect their information from errors that could be caused by the deliberate actions of disgruntled employees or by unintentional accidents. The error dimension arises from non-deletion (not forgetting) of old data, as old data can become "erroneous" because of their static nature in a dynamic world [64]. Smith et al. [86] suggested that companies should provide the "edit" functionality to overcome error concerns but did not offer any recommendation regarding the deletion of old data.

Control: Control over the collection and usage of personal information is a key factor in explaining privacy concerns [84]. A lack of control

Table 1
Salient privacy concern scales.

Source	COL	SEC	UNA	ERR	AWA	CON	RTBF	OVE	Theory	PC factor structure	Comments
Dinev and Hart [31]	X	X	X					X	Privacy calculus	First-order factor structure with two independent dimensions – information finding and information abuse. Abuse comprised secondary use and unauthorized access. Finding comprised monitoring and collection.	Collected data from undergraduate and graduate students, organization employees, and general public
Earp et al. [34]	X	X	X		X			X	Fair Information Practice Principles	First-order factor structure with six dimensions: personalization, collection, transfer, notice/awareness, storage, and access/participation.	The survey was distributed online to Internet users worldwide
Hoehle et al. [41]	X	X	X	X					MDT	Two second-order factors: information management (unauthorized access and errors) and interaction management (collection and secondary use concern).	Recruited participants from a mailing list maintained by a retail laboratory
Hong and Thong [44]	X	X	X	X	X	X			MDT	Third-order factor structure with two second-order factors of interaction management (i.e., with collection, secondary use, and control as its first-order factors) and information management (i.e., with unauthorized access and errors as its first-order factors), and a first-order factor, awareness.	Survey was advertised on the homepage of a Hong Kong website
Malhotra et al. [57]	X				X	X			Social Contract and Justice	Second-order factor structure with three first-order dimensions (i.e. collection, control, and awareness).	Conducted two separate field surveys and collected data from 742 household respondents in one-on-one, face-to-face interviews
Smith et al. [86]	X	X	X	X					Fair Information Practice Principles	A correlated set of four first-order dimensions: collection, error, unauthorized secondary use, and improper access.	Recruited a diverse pool of respondents: students, executives and organizational employees, consumers, and judges
Steinbart et al. [90]	X	X	X	X	X	X	X		Generally Accepted Privacy Principles [3]	Third-order factor with two second-order factors – interaction management and information management. Identified RTBF as a distinct construct, alongside six other dimensions of PC; couldn't settle on how RTBF relates to the other six PC dimensions.	Amazon MTurk and students
Stewart and Segars [92]	X	X	X	X					Concern for Information Privacy [86]	Second-order factor structure with four first-order dimensions – collection, unauthorized access, errors, and secondary use.	Data for model testing were obtained through a survey of 400 consumers
Xu et al. [106]		X	X					X	Communication Privacy Management (CPM)	Second-order model comprising three first-order dimensions (i.e., perceived surveillance, perceived intrusion, and secondary use of personal information).	Recruited undergraduate and graduate students at a US university
Current study	X	X	X	X	X	X	X	X	MDT	We built upon the work of Hong and Thong [44] to incorporate RTBF and OVE into the existing frameworks for PC.	Amazon MTurk

Note: COL = collection, SEC = secondary use, UNA = unauthorized access, ERR = error, AWA = awareness, CON = control, RTBF = right to be forgotten, OVE = oversight from surveillance, PC = privacy concern, MDT = multidimensional development theory

increases online consumers' privacy concerns [57]. Citing Stone et al. [94], Smith et al. [86] referred to information privacy as the ability of an individual to personally control information about oneself. Control is associated with fairness [57] as well as the ability to prevent subsequent misuse of one's personal information [28]. The issue of control becomes more pronounced when there exists opportunistic behavior to benefit from users' information.

Awareness: Awareness refers to a combination of three aspects: (1) literacy in the elements related to information privacy, such as technology, regulations, or common practices used by companies to collect, use, and share users' information; (2) the understanding that these elements exist in the current environment; and (3) the projection of the impact of these elements in the future [24]. This dimension of privacy concerns refers to the degree to which a person is concerned about his/her awareness of information privacy practices [44, 57]. Hong and Thong [44] have demonstrated that awareness is a passive dimension of privacy concerns [57, 65]. Accordingly, the awareness factor is highly interrelated with, but distinct from, other privacy dimensions [84].

RTBF: The RTBF stems from the concern for removing outdated information – for example, references to the crimes committed by a criminal after he or she has served the sentences and taken corrective actions [17]. Several privacy advocates note that the RTBF would allow children and youth to erase information posted improvidently. Arguing in favor of the RTBF, Bennett [17] noted that the concept of "forgive and forget" embodies a fundamental human value and that US laws (e.g., relating to bankruptcy, credit reporting, and crimes) recognize some

Table 2
Privacy concern dimensions

Dimension	Definition	Source
Collection	The degree to which an individual is worried about the amount of his/her personal information that is collected	Smith et al. [86]
Unauthorized/improper access	The degree to which an individual is concerned about his/her personal information being made readily available to unauthorized parties	Smith et al. [86]
Secondary use	The degree to which an individual is concerned about the unjustified use of his/her information for purposes other than those for which they were initially gathered	Smith et al. [86]
Errors	The degree to which an individual is concerned about the deliberate or unintentional errors that might be made to his/her personal information	Smith et al. [86]
Control	The degree to which an individual has control over how his/her information is used	Hong and Thong [44]
Awareness	The degree to which an individual is adequately aware that his/her information is being collected	Hong and Thong [44]
Right to be forgotten	The degree to which an individual is concerned that his/her past information in the post-use context would never be erased	Steinbart et al. [90]
Oversight from surveillance	Concerns about the monitoring of users' Internet activity	Dinev et al. [33]

elements of the right for individuals' past information to be forgotten. Even though the RTBF is not recognized as a legal right of the citizens in the USA, given the increasing surveillance, people are concerned that the lack of RTBF protection can damage their information privacy [61].

Critiques of the RTBF in the USA argue that it would create a bureaucratic nightmare that might interfere with business demands for data and is not constitutionally valid [53]. Despite difficulties in implementing the RTBF, scholars have pointed out how it needs to be implemented globally [70] and acknowledged that the degree of rights could vary across countries, thus complicating its implementation. Villaronga et al. [102] argued that the RTBF could have various meanings and implications, such as (a) simple removal from the search index, (b) overwriting data in the file system, (c) deletion from log files and backups, and (d) removal from all internal mechanisms.

To date, there has been limited research in the IS area on the RTBF. Table 3 summarizes legal reviews and theoretical papers that have debated the issue of the RTBF. The debate about whether the USA should make the RTBF a regulatory requirement is unsettled. Several researchers have argued for legalizing the RTBF in the USA [e.g., 17, 58], whereas others have argued against it because of the US Constitution's First Amendment [53]. Table 3 presents a summary of the research on the RTBF.

Oversight from surveillance: Information technology has enabled a greater capacity for computation, storage, and retrieval, but it has also provided the means for surveillance and exploration (e.g., data mining). Internet technology provides an almost unprecedented opportunity for the unobtrusive surveillance of information related to personal interests [25, 27]. In the post-9/11 world, security concerns rule over privacy concerns, giving rise to surveillance [31]. Surveillance has been defined in law journals as "the watching, listening to, or recording of an individual's activities" [86, p. 490], which is very similar to the definition provided by the World Health Organization as the "systematic ongoing collection, collation, and analysis of data and the timely dissemination of information to those who need to know so that action can be taken"

Table 3
Salient literature review on the right to be forgotten

Source	Journal	Research methodology	Findings
Bennett [17]	*Berkeley J. Int'l Law*	Legal review	Argued that various US laws, including bankruptcy laws favoring fair information practices, do accept some version of the RTBF, and presented a thoughtful reflection on how the US's and EU's views on the RTBF can be reconciled.
Bygrave [20]	*Communications of the ACM*	Theoretical paper	Contrasted EU data privacy regulations with those of the US, and speculated on the role of US-based search engines such as Google in complying with EU privacy laws which, unlike the US, treat information privacy on the same par as a fundamental right.
Kwak et al. [52]	*Americas Conference on Information Systems*	Theoretical paper	Argued that data controllers should devise procedures to provide objective evidence of the disposal processes of user data to assure the user that his/her request to erase his/her past has not been forgotten.
Larson III [53]	*Communication Law and Policy*	Legal review	Demonstrated how the idea of the RTBF is fundamentally at odds with the right of freedom of speech and the US's First Amendment.
Mantelero [59]	*Computer Law & Security Review*	Legal review	Provided an overview of boundaries of the RTBF as defined by the US courts using two different legal cases: *Melvin v. Reid* and *Sidis v. F-R Publishing Corporation*. It suggested that the US does not hold the right to be forgotten as entirely foreign. It also argued for the active role of regulation to ensure not only one's fundamental rights but also the freedom of expression.
Newman [70]	*Science*	Theoretical paper	Argued that to implement the RTBF locally in the EU, it needs to be enforced globally, as information flows routinely across the borders.
O'Hara [71]	*IEEE Internet Computing*	Theoretical paper	Discussed the pros and cons of the RTBF, the arguments presented by Google Spain to avoid taking responsibility for protecting the RTBF and how the EU argued and set the search engine's responsibility in ensuring the RTBF.
Steinbart et al. [90]	*50th Hawai'i International Conference on System Sciences*	Research survey. Two pilots were conducted with Amazon MTurk, and one pilot was conducted with students	Scale development to measure individuals' concerns about the RTBF.
Villaronga et al. [102]	*Computer Law & Security Review*	Theoretical paper	Argued that it may be impossible to fulfill the legal aims of the RTBF, as deletion could mean (a) simple removal from the search index, (b) overwriting in the file system, (c) deletion from log files and backups, and (d) removal from all internal mechanisms. Made a case for pursuing more interdisciplinary studies supporting privacy law and regulation.

[105]. Thus, even though surveillance is fueled by data collection and secondary usage, it is different in that surveillance refers to *continuous* and *systematic* monitoring and scrutiny with specific purposes in mind (i.e., action oriented) and can be associated with primary or secondary use. Surveillance, like persistent gawking, can cause feelings of anxiety and discomfort [87]. Interestingly, as information becomes more private and personal, the desire for others to acquire it, for both noble and inappropriate reasons, increases [4, 63]. Concerns on surveillance and oversight come into play as organizations increasingly fail to restrict unauthorized secondary use by the government or businesses while increasing the degree of tracking and profiling of their clients or customers. Smith et al. [86] advised that to reduce unauthorized secondary use concerns, corporations should "refuse to release personal data to outside entities" (p. 192). Companies such as Google and Facebook comply with the vast majority of the data requests by the US government regarding individuals, and as data become concentrated with a few big technology companies, it becomes easier for the government to get access to individuals' data, thus fueling even greater concerns with surveillance and oversight. The literature provides justifications and raises awareness that surveillance concerns need to be voiced actively [49].

So, why is surveillance increasing, and in what ways is it related to privacy concerns? Flaherty [35] argued that companies and government agencies are under intense pressure to reduce costs, promote efficiency, and spend public money wisely. Surveillance technology appears to be a neutral, objective process that can be wielded as a weapon, or at least a tool, against welfare cheats (targeting those on income assistance), sex offenders (targeting those who work with children through criminal-record checks), and speeders (radar monitoring all cars and photographing the license plates of speeders). Friedman and Reed [36] argued that the increasingly competitive business environment, legislation to protect employers' interests, new technologies that enhance employers' ability to monitor electronic communications, and the need for businesses to avoid costly lawsuits have fueled surveillance. Bellaby [16] provided two important reasons for the increase in surveillance: backdoors and web crawlers. The capability of technology companies to capture rich and highly contextual phone data has prompted government intelligence agencies to ask, or even force, technology companies to build backdoors into their devices and programs to allow access to consumer data as needed. These *backdoors* lower the bar to allow surveillance en masse. *Web crawlers* have provided governments with the ability to scan web activities automatically to identify patterns and detect any possible threats. Bellaby [16] argued that corporations and states are unlikely to instigate a change that would significantly limit their intelligence collection activity in their pursuit to drive profitability and efficiency.

Several privacy advocates and researchers have expressed arguments that explain how surveillance concerns with government and corporate firms are associated with privacy concerns. Advances in technology that create benefits for both consumers and organizations are also raising privacy concerns because of the potential for surveillance [27]. Government surveillance can infringe personal privacy [23] and lower user trust [25]. Surveillance concerns, like other privacy concerns, can lower the willingness to share information [30, 33, 106]. Dinev and her colleagues [30, 33] showed that government intrusion concerns are positively related to privacy concerns which, in turn, are negatively related to the willingness to provide personal information over the Internet. Several studies have argued that such concerns lower privacy self-efficacy [58] and intention to share information online [e.g., 33, 72].

Privacy intrusion by corporate surveillance [103] and government surveillance pose similar concerns to citizens [16, 40]. Smith et al. [86] mentioned the "Big Brother" effect as a tangential privacy concern factor. Stone-Romero et al. [93] have shown that surveillance and oversight/monitoring practices which include personality inventories, background checks, lie detection, biographical inventories, covert surveillance, drug testing, telephone monitoring, and electronic monitoring of work and Internet use heighten privacy concerns. In the organizational context, surveillance and monitoring systems can invade personal boundaries, resulting in perceptions of privacy invasion and fairness issues [109]. Kurkovsky and Syta [51] presented the results of a study on the use of electronic communications by college students at public universities in which users adjusted their communications in response to the possibility of diminishing privacy and their understanding of the privacy policies. Earp et al. [34] also indicated that monitoring by websites to increase personalization is related to one of the privacy concern factors. Ariss [5] examined the impact of corporate monitoring on employee productivity and argued that random monitoring can boost productivity; however, excessive "snoopervision'' may be regarded as unethical and economically destructive. Drawing on the work by Botan [19], D'Urso [29] suggested that perceived concerns for surveillance may moderate how individuals perceive electronic monitoring practices and policies within an organization.

Several papers have discussed oversight from surveillance in the context of privacy concerns (see Table 4); however, systematic empirical research that examines privacy dimensions associated with surveillance concerns is lacking. Bélanger and Crossler [15] stated that surveillance is less frequently researched or recognized as a privacy concern.

Table 4 provides an overview of salient research in the area of surveillance.

Drawing on the work by Hong and Thong [44], we adopted the MDT to conceptualize the IPC construct [54]. Based on MDT, IPC was conceptualized by Hong and Thong [44] as a multidimensional construct that comprises self-development, environmental impact, and interpersonal interaction that can be further broken down into interaction management and information management, as well as the ability to perceive choices (i.e., awareness). Self-development and environmental impact are related to how privacy concerns develop over time, where environmental impact emphasizes the need to reevaluate the construct over time [37]. In the context of information privacy, information management refers to how well personal information is managed (i.e., in the database or data repository of some form), and interaction management refers to the ability of the owner to manage the "collection and subsequent use of his or her personal information by websites" (p. 277). Hence, the former is concerned about the management of data (i.e., personal information) per se, and the latter is concerned about the interaction of the data (i.e., personal information) with others that is beyond data management.

Based on the findings by Hong and Thong [44], IPC is conceptualized as a third-order construct comprising two second-order constructs, information management (unauthorized/improper access and errors) and interaction management (collection, secondary use, and control), and a separate first-order construct, awareness. Based on MDT and the conceptualization of IPC by Hong and Thong [44], oversight from surveillance is related to managing the collection and use of one's information for monitoring purposes, and hence, describes a type of interaction management.

The classification of the RTBF using the dimensions of MDT, however, is less clear, as observed and articulated by Steinbart et al. [90]. The RTBF refers to the last stage of dealing with one's personal information, where the information is no longer relevant and, hence, should be discarded or disposed of by the party that collected the information. Laufer and Wolfe [54] identified two distinct elements of privacy concerns beyond self-development, environmental impact, and interpersonal management. One of these elements refers to the ability to perceive options (i.e., awareness), and the other refers to the ability to exercise choices over the options, which directly relates to the RTBF. The RTBF refers to whether one has the right or ability to dispose of or discard one's personal information. Hence, the RTBF is a separate factor that is not part of information management or interaction management. Next, we will draw on the conceptualization of the IPC model by Hong and Thong [44] and analyze the inclusion of two new dimensions, oversight from surveillance and the RTBF, into the model.

Table 4
Salient literature review on surveillance

Source	Journal	Research Methodology	Findings
Agre [2]	*The Information Society*	Opinion paper	Compared two models of privacy: surveillance and capture models. The surveillance model is based on secret police state, whereas the capture model is based on computer tracking by organizations in real time. Argued that these models are not mutually exclusive.
Bellaby [16]	*Ethics and Information Technology*	Opinion paper	Argued that due to the en masse surveillance – from both governments and corporations – coupled with people's limited awareness and ability to comprehend such data collections, anonymizing technology should be built into the fabric of cyberspace to provide a minimal set of privacy protection to individuals.
Crossler and Posey [25]	*Journal of the Association for Information Systems*	Survey on Amazon's Mechanical Turk	Argued that in an environment with potential privacy issues such as future monitoring and surveillance activities, trustworthiness factors are paramount in individuals' privacy protection technology adoption decisions.
Dinev et al. [30]	*Journal of Global Information Management*	Survey of 889 participants from Northern Italy and 422 participants from the southeastern US	Examined the relationships of privacy concern, need for government surveillance, and concern for government intrusion on e-commerce use for two countries: Italy and the USA.
Dinev et al. [33]	*Journal of Strategic Information Systems*	Survey of 422 individuals in southeastern US states	Examined the relationships of Internet privacy concern, need for government surveillance, and concern for government intrusion on willingness to provide personal information to transact on the Internet.
Earp et al. [34]	*IEEE Transactions of Engineering Management*	Content analysis	Developed a taxonomy of 12 categories for two privacy goals: privacy-protection goals and privacy-vulnerability goals. Identified information monitoring as a privacy-vulnerability goal.
HLR [40]	*Harvard Law Review*	Legal review	Argued that technology companies have turned into "surveillance intermediaries" that have the power to decide just how easy or difficult it will be for law enforcement to access user information stored with these companies.
Joh [49]	*Arizona Law Review*	Legal review	Argued that US Constitution's Fourth Amendment law makes little distinction between ordinary criminal evasions and privacy protests – where citizens object to government surveillance. The article describes the importance of individuals' objection to surveillance and why it should be treated differently than surveillance evasion.
Kim [50]	*International Sociology*	Opinion paper	Analyzed the dynamic relationship between surveillance technology and social control. They argued that technological advancement in surveillance technology leads to diffusion and enhanced acceptance of surveillance in the society, which, in turn, leads to an increase in demand for surveillance technology. As surveillance becomes more accepted in society, it also changes the concept of privacy in the society.
Kurkovsky and Syta [51]	*Hawaii International Conference on System Sciences*	Survey of 65 students	Presented results of a study on the use of electronic communications by college students at public universities. As a result of their understanding of the policies, users often adjust their communications in response to the possibility of diminishing privacy.
Mamonov and Koufaris [58]	*Journal of Information Privacy and Security*	Survey of 483 respondents from Amazon MTurk	Found that exposure to news about government surveillance increases the level of concern about government intrusion and decreases privacy self-efficacy, which leads to users using weaker passwords.
Marthews and Tucker [60]	SSRN 2412564	Panel data from the US and its top 40 trading partners on the search volume of select keywords from before and after the surveillance revelations of June 2013	Showed that the US government surveillance programs may damage the economic profitability of US-based Internet firms relative to non-US-based Internet firms.
Miltgen and Smith [66]	*Information & Management*	Online survey of 925 respondents from the UK	Argued that most of the consumer concerns associated with surveillance were being directed more at commercial than governmental data interchanges. It developed and tested a consolidated model that addressed a number of constructs related to governmental regulations associated with users' information on the Internet.
Mitsilegas [67]	*Tilburg Law Review*	Legal review	Highlighted the transformation of the right to privacy by judiciaries in Europe to counter generalized, massive pre-emptive surveillance in the EU, the USA, and globally.
Oulasvirta et al. [73]	*Cyberpsychology, Behavior, and Social Networking*	Online experiment with 1,897 respondents	Analyzed how data disclosure practices in ubiquitous surveillance affected users' privacy concerns and intentions to share information. Intentions were moderated by the collectors' identity and intention disclosure.
Reddick et al. [79]	*Government Information Quarterly*	Political discourse analysis of #NSA tweets and data from Pew research surveys	Indicated that government needs to be more efficacious in communicating about surveillance programs more transparently to garner greater citizen approval for its surveillance programs.
Regan and Jesse [80]	*Ethics and Information Technology*	Theoretical paper	Identified six ethical concerns raised by big data: information privacy (collection), anonymity, surveillance, autonomy, non-discrimination, and ownership of information.
Semitsu [81]	*Pace Law Review*	Legal review	

(*continued on next page*)

Table 4 (*continued*)

Source	Journal	Research Methodology	Findings
			Using the Supreme Court ruling, it argued that what a person knowingly exposes to the public (as in the case of Facebook) is not a subject of Fourth Amendment protection, and Facebook users cannot expect federal law to stop their private content and communications from surveillance and from their information being used against them.
Sharma and Crossler [83]	*Electronic Commerce Research and Applications*	Survey of 252 students	Analyzed the effect of perceived surveillance on perceived risk in the social commerce environment.
Smith et al. [86]	*MIS Quarterly*	Privacy concern scale development	Argued that the "Big Brother" effect is a tangential privacy concern factor.
Solove [87]	*Pennsylvania Law Review*	Legal review	Indicated that continuous monitoring as surveillance has problematic effects, which can create feelings of anxiety and discomfort.
Stoycheff [95]	*Journalism & Mass Communication Quarterly*	Survey of 255 individuals recruited by a commercial survey firm, SSI	Perceptions of surveillance practices limit the sharing of opinions and information by the minority-opinion groups.
Thompson et al. [97]	*Journal of the Association for Information Science and Technology*	An online survey of 242 Australian and Sri Lankan residents	Found that respondents conflate surveillance with the collection of data and may not consider subsequent secondary use.
Verble [100]	*SIGCAS Computers & Society*	Opinion paper	Examined the case and background of Edward Snowden, the history and purpose of the National Security Agency (NSA), legality, and American public opinion and its aftermath.
West [103]	*Business & Society*	Analysis of secondary data	Examined how the advent of commercial surveillance is centered around the idea of "data capitalism" to make a profit.
Xu et al. [106]	*Thirty-Third International Conference on Information Systems*	Survey of 310 students	Developed the mobile users' information privacy concerns (MUIPC) scale comprising three dimensions: perceived surveillance, perceived intrusion, and secondary use of personal information.
Yang and Lin [107]	*Journal of Electronic Commerce Research*	Survey of 451 users of social-local-mobile (SoLoMo) services	Found that three stressors – information overload, social message overload, and perceived surveillance – significantly impact users' anxiety.

3. Research Methodology

Data were collected using the Qualtrics survey from Amazon Mechanical Turk (MTurk). Three hundred and twelve people in the USA completed the survey, and 275 of them passed the attention check questions. The final sample has an average age of 34 years, with a standard deviation of 10 years. The age of the participants ranged from 18 to 69 years. There were 155 males and 119 females; one person chose "other" for gender. Of the sample, 95% had attended college or higher education. Seventy-seven percent were employed full-time, 10% were employed part-time, and 10% were self-employed.

3.1. *Measurement*

We used available preexisting scales and developed items for constructs that are not available in the literature, as shown in Table 5. The measurement items are provided in Appendix A.

We adopted the IPC model from Hong and Thong [44] with unauthorized access (UA) and errors (ERR) as information management; control (CON), collection (COL), and secondary use (SEC) as interaction management; and awareness (AWA) as a first-order factor. In addition, as justified earlier, oversight (OVE) is a type of interaction management, and the RTBF is a separate first-order factor. Using the proposed measurement model generated based on theorization provided by Hong and Thong [44], we assessed the proposed IPC model in the context of the research model presented in Fig. 1 (Model 2) along with the baseline model where all factors are presented in a first-order model (Model 1); see Table 6. Hence, we compare our proposed model (Model 2) with the baseline model (Model 1) that has all eight dimensions as first-order factors.

Table 5
Measurement instrument

Construct	Adapted from
Concern with collection Concern with secondary use Concern with unauthorized access Concern with errors	Awad and Krishnan [9]; Bansal et al. [11]; Dinev and Hart [32]; Hong and Thong [44]; Malhotra et al. [57]
Awareness	Hong and Thong [44]; Steinbart et al. [90]
Right to be forgotten	Steinbart et al. [90]
Control	Hong and Thong [44]; Steinbart et al. [90]
Oversight from surveillance	Self-developed
Trust in the Internet	Bélanger and Carter [14]
Trust in online businesses	Bélanger and Carter [14]; Teo et al. [96]
Trust in government	Bélanger and Carter [14]; Teo et al. [96]

We conducted reliability analysis (as shown in Table 7) as well as discriminant and convergent validity analysis (as shown in Table 8) based on the proposed model (i.e., model 2 in Table 6). The constructs demonstrated adequate reliability (Table 7) with Cronbach's alpha coefficients greater than 0.7 for all of them. Table 8 shows the construct correlations with the diagonal presenting square root of AVE. Construct correlations (Table 8) are less than the square root of AVE, demonstrating support for discriminant validity. AVE values are greater than 0.5, thus demonstrating support for convergent validity. We also found support for convergent and discriminant validity through exploratory factor analysis. The loadings on the intended factors are all greater than 0.7, indicating good convergent validity, and the cross-loadings are less than 0.4, demonstrating good discriminant validity.

We also examined the measurement model (based on the proposed model, i.e., model 2) using Mplus [68]. The fit indices for the confirmatory factor analysis model meet the generally accepted thresholds (see Table 9), further demonstrating adequate measurement fit. The fit indices for the estimation models (see Table 10) also fall within recommended thresholds (as discussed later), indicating adequate model fit.

We also checked the common method bias (CMB) using two different methods. We used the Harman test and found that the first factor explains 29.47% of the variance, which is less than 50%, suggesting that CMB is not a serious threat. Secondly, following Lindell and Whitney [55], we used the second-lowest positive correlation between a marker variable (i.e., a variable not related to any aspect of this research) and the first-order factors in this research as a conservative estimate of shared correlation resulting from common method variance. We used a prior marker variable ("I really get involved with the feelings of the

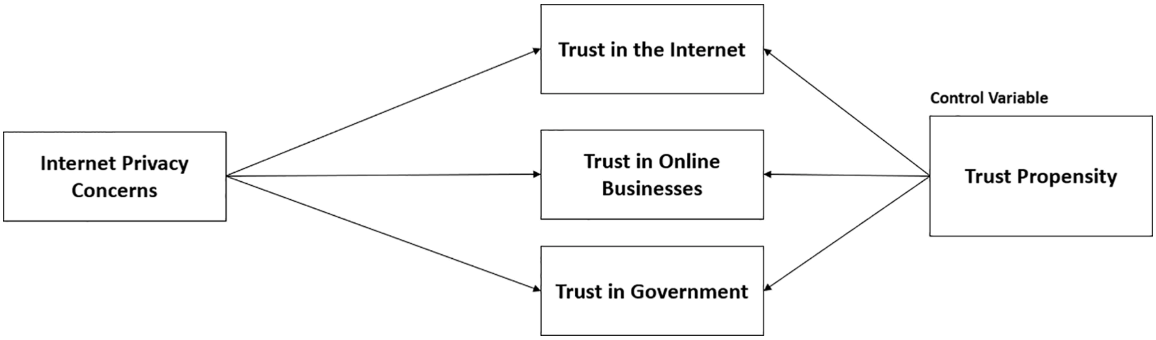

Fig. 1. Research model

Table 6
Model comparison

Model 1 (baseline)	First-order model comprising all eight dimensions: UA, ERR, COL, SEC, OVE, CON, RTBF, and AWA
Model 2 (proposed)	Information management (second-order – UA and ERR) Interaction management (second-order – COL, SEC, CON, and OVE) First-order factors - AWA, RTBF

UA – unauthorized access, ERR – error, COL – collection, SEC – secondary use, CON – control, AWA – awareness, OVE – oversight from surveillance, RTBF – right to be forgotten

Table 7
Reliability analysis

Construct	Cronbach's alpha	Composite reliability	Average variance extracted (AVE)
UA	0.83	0.92	0.85
ERR	0.78	0.90	0.82
COL	0.81	0.89	0.73
SEC	0.85	0.91	0.77
CON	0.79	0.88	0.71
AWA	0.78	0.87	0.70
OVE	0.77	0.90	0.81
RTBF	0.85	0.91	0.77
Information Mgmt	0.85	0.90	0.69
Interaction Mgmt	0.91	0.92	0.53
IPC	0.95	0.96	0.50
TRINT	0.84	0.90	0.76
TROB	0.84	0.90	0.76
TGOV	0.84	0.93	0.82
TRPR	0.87	0.92	0.79

Note: UA – unauthorized access, ERR – error, COL – collection, SEC – secondary use, CON – control, AWA – awareness, OVE – oversight from surveillance, RTBF – right to be forgotten, IPC – Internet privacy concerns, TRINT – trust in Internet, TROB – trust in online businesses, TGOV – trust in government, TRPR – trust propensity

characters in a movie") and computed the correlations. The second-lowest positive correlation score was 0.011, which was low and insignificant [44], suggesting that CMB is not a serious threat.

To analyze the conceptualization of the IPC model comprising the eight dimensions – collection, unauthorized access, secondary use, errors, control, awareness, oversight, and the RTBF – we assessed the IPC model in the context of trusting beliefs using the model as shown in Fig. 1. In addition to capturing the eight dimensions of IPC, we also assessed the respondents' trusting beliefs in the Internet, online businesses (in general), and government. Hence, we assessed the new IPC construct comprising eight dimensions within a nomological network that includes trusting beliefs (see Fig. 1).

4. Data Analysis

Table 10 shows the results of the fit indices of the estimation models, computed using the nomological network as shown in Fig. 1, as well as the R squares from the research model (see Fig. 1) for Model 1, Model 2, and Hong and Thong's [44] model constructed using six dimensions (information management: UA and ERR; interaction management: COL, SEC, and CON; AWA as an independent first-order factor). The results indicate that Model 2 has better fit indices and substantially higher R square values for the trust constructs than Model 1. Model 2 also explains higher variability in the trust variables as compared to the original model from Hong and Thong [44].

The structure of IPC from Model 2 is shown in Fig. 2. We also show the factor loadings and t-statistics computed for Model 2 in Fig. 2 for the higher-level constructs, and in Table C1 of the Appendix for lower-level constructs. The factor loadings are all significant with t-value greater than 1.96. The path coefficients and t-statistics of the structural model for model 2 are shown in Fig. 3. The path coefficients show that IPC lowers trust in Internet and government, but not trust in online businesses, whereas trust propensity, as expected, increases trust in all three entities – i.e., Internet, online businesses, and government. We computed path coefficients with alternate IPC models (as shown in Table B4 of the Appendix) and found the path from IPC to online businesses to be insignificant. It is possible that when trust in the Internet and government are present in the model, the path to trust in online businesses becomes less salient.

5. Discussion and Conclusion

Prior research on privacy has established that people are concerned about the collection of data, secondary use of data, unauthorized access to data, and erroneous data. They are also concerned about the degree to which they can control what organizations or governments can do with their information, oversight of their information by government surveillance, concerns about the ability to delete their information, and awareness about the security of their information. This study proposes and investigates the inclusion of privacy concerns associated with oversight from surveillance and the RTBF as additions to the existing IPC scale developed by Hong and Thong [44]. The study compares our proposed eight-dimensional IPC model with a baseline model (with all eight dimensions as first-order factors) and demonstrates that the proposed model has a better empirical and theoretical structure to explain and represent IPC. The proposed third-order IPC model has two second-order factors – information management (comprising unauthorized access and errors) and interaction management (comprising collection, secondary use, and oversight concerns) – and two independent factors, awareness and the RTBF.

Since IPC is a dynamic construct, we need to constantly evaluate and update the IPC model and instrument as and when major changes that can impact data usage are observed [37]. The IPC scale needs to be periodically updated, especially after significant social and

Table 8
Construct correlation matrix (with square root of AVE on the diagonal)

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1 COL	0.85														
2 CON	0.58	0.84													
3 ERR	0.55	0.49	0.91												
4 INFO	0.55	0.62	0.90	0.83											
5 INTER	0.83	0.88	0.61	0.72	0.73										
6 OVE	0.65	0.64	0.51	0.56	0.79	0.90									
7 IPC	0.74	0.88	0.71	0.84	0.96	0.74	0.71								
8 RTBF	0.55	0.79	0.53	0.64	0.79	0.61	0.87	0.88							
9 SEC	0.57	0.71	0.52	0.67	0.84	0.48	0.84	0.68	0.88						
10 TGOV	-0.12	-0.26	-0.02	-0.12	-0.24	-0.18	-0.24	-0.23	-0.25	0.91					
11 TRINT	-0.09	-0.19	-0.01	-0.10	-0.19	-0.16	-0.18	-0.12	-0.18	0.72	0.87				
12 TROB	0.01	-0.02	0.06	0.02	-0.01	0.00	0.00	0.01	-0.02	0.65	0.72	0.87			
13 TRPR	0.05	-0.02	-0.06	-0.09	-0.02	-0.04	-0.05	0.00	-0.05	0.60	0.56	0.48	0.89		
14 UA	0.46	0.64	0.66	0.92	0.70	0.50	0.81	0.64	0.70	-0.19	-0.16	-0.02	-0.11	0.92	
15 AWA	0.54	0.77	0.56	0.70	0.77	0.56	0.87	0.73	0.68	-0.23	-0.20	0.00	-0.07	0.70	0.84

Table 9
Measurement models

Fit indices	Chi sq / df	CFI	TLI	RMSEA	SRMR
Model 1 CFA	777.137/477	.924	.915	.049	.059
Model 2 CFA	756.357/475	.928	.920	.048	.060

Table 10
Estimation models

Fit indices	Model 1 (base)	Model 2 (proposed)	Hong and Thong's six-dimension model
Chi sq / df	777.156/ 477	754.071/475	552.065/332
CFI	.924	.929	.931
TLI	.915	.921	.922
RMSEA	.049	.047	.050
SRMR	.056	.055	.057
Rsquare TRINT	.441	.458	.443
Rsquare TROB	.338	.352	.348
Rsquare TGOV	.533	.544	.525

technological changes that impact secondary usage or unauthorized monitoring of data, which may impact Internet users' privacy perceptions [44]. Xu et al. [106], in their reply to a self-posed question on why more research on measurement for privacy concerns is needed, argued that instruments are needed as technology and its usage change. It becomes important to capture the dimensions proposed in this paper – concerns due to oversight from surveillance and the RTBF, as they are not covered (or at least not adequately covered or explicitly represented) by the existing dimensions. As the law catches up (see [82] for RTBF-related legal changes in the USA and [46] for their changing surveillance landscape in the USA), the scale needs to catch up as well.

Finally, our results provide support for the conceptualization of the RTBF as a unique passive dimension of IPC. The RTBF is somewhat independent of the other dimensions, because no matter what interaction management or information management practices are adopted by a website, the website may or may not allow individuals to remove their past history. Hence, individuals' information privacy could be infringed without altering the interaction management and information management practices of the websites. The RTBF, just like awareness [44], constitutes a unique dimension in addition to the interaction management and information management dimensions.

5.1. *Why is Model 2 Theoretically and Empirically Superior?*

Model 2 (Fig. 2) depicts IPC as a third-order model with two second-order factors, information management and interaction management, and two first-order factors. Information management comprises two first-order constructs, unauthorized access, and errors, whereas interaction management comprises four first-order constructs: collection, secondary use, control, and oversight. Next, we provide further theoretical arguments that support oversight as an interaction management

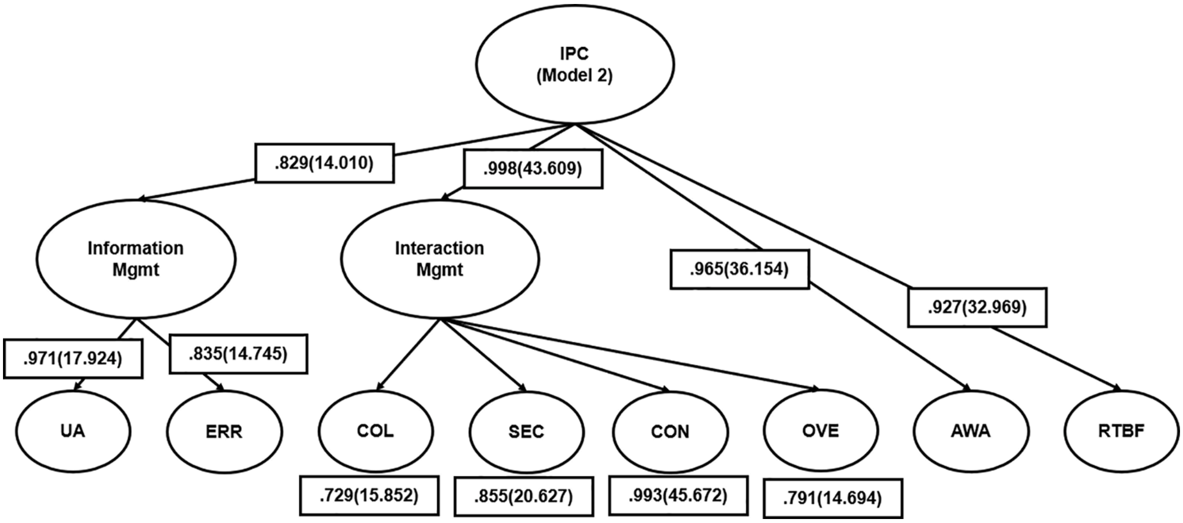

Fig. 2. Emergent IPC structure (Model 2) with factor loadings and t-statistics

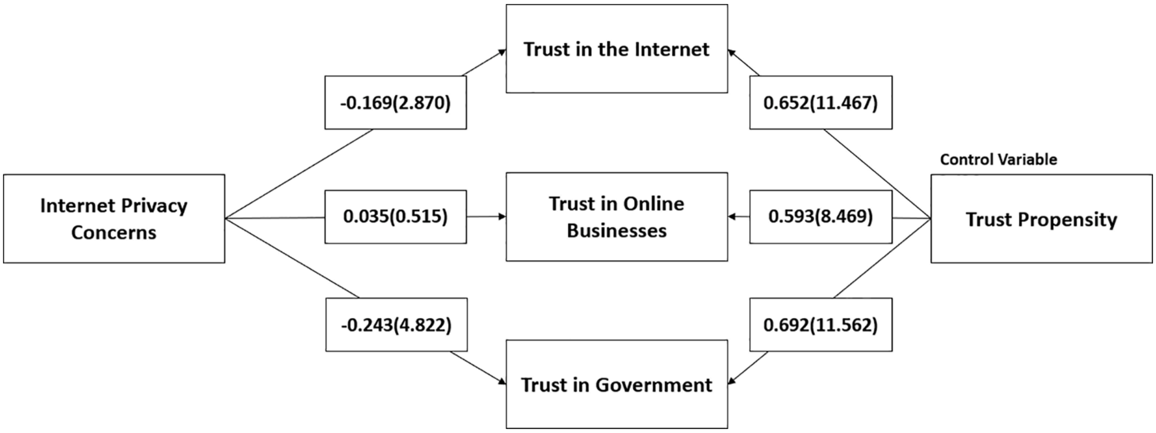

Fig. 3. Results (using Model 2)

dimension and the RTBF as an independent first-order construct.

(1) Association of oversight from surveillance, collection, and secondary use concerns with interaction management: The majority of users in the USA are aware of government oversight, and some are very concerned about it. The Pew Research Survey conducted in late 2014 and early 2015 reported that 87% of Americans indicated that they had heard about the government surveillance programs, and 57% of Americans said it was unacceptable for the government to monitor the communications of US citizens [39]. Surveillance and oversight concerns arise from the collection of data and hence, are associated with interaction management. Dinev and Hart [31] and Earp et al. [34] argued that monitoring represents a form of data collection from Internet users. Xu et al. [106] pointed out that surveillance is rooted in collection and suggested that aggressive data collection, particularly due to the widespread use of smartphones, has promoted massive data collection and fueled the impression that vendors are constantly monitoring user behavior through smartphones. The collection and combing of data and using data for secondary purposes suggest a “Big Brother” environment [86] (p. 174).

(2) Association of oversight from surveillance and control with interaction management: Concerns associated with oversight from surveillance, control, collection, and secondary usage share some common variance which can be explained by a higher-order dimension – interaction management. Control helps lower privacy concerns by creating boundary structures that reduce the amount of information collected by others [22, 74, 106]. Suggesting that surveillance and oversight concerns share some association with lack of control, Sheehan and Hoy [84] argued that as multiple entities (such as government) get involved in sharing consumer (or citizen) information, consumers lose control, and concerns with privacy increase.

(3) The RTBF is an independent factor: Based on the evidence presented in this research, it could be argued that the RTBF is independent of information and interaction management dimensions. In the USA, the RTBF is a passive concern. There are many users who are concerned about information privacy and support the RTBF [17] but also believe that the First Amendment trumps the RTBF [53]. Regardless of the interaction and information practices used, the RTBF could be implemented or not implemented by a website vendor or owner. It is similar to awareness in which “no matter what interaction management or information management practices are adopted by a website, it can choose to let individuals be aware of it or not” [44]. Some individuals in the USA might desire to have the RTBF, but it is not enforced and, hence, is not a mandatory component of information or interaction management. Awareness and the RTBF are two sides of a coin. Awareness refers to the ability to know whether one’s personal information is collected and how it is used, whereas the RTBF refers to the ability to determine whether one’s personal information will be deleted or not. Thus, Model 2 supports the notion that awareness and the RTBF are both passive and independent of other dimensions of IPC.

In the future, if the RTBF evolves to be a more active concern, particularly in the US and also elsewhere, it will be important to examine if it aligns with interaction management, since RTBF pertains to individual’s control [90] over whether his/her information can be erased, and thus might evolve to be part of interaction management which deals more specifically with the ability of an individual to manage the collection and subsequent use of his or her personal information by websites [44]. As RTBF evolves to become an increasingly important privacy concern or even an individual’s right, it is possible to become subsumed under interaction management.

We carried out an extensive post-hoc analysis contrasting various combinations of the eight IPC dimensions studied in this paper, as shown in Appendix B (Tables B1–B4). The detailed statistical analysis combined with the theoretical support reinforces the superiority of Model 2.

5.2. Implications for Theory

The findings have several major theoretical implications. First, adding the oversight and RTBF dimensions to the IPC scale addresses the need and concerns expressed in the literature [21, 38]. The paper answers the call by Hong and Thong [44] by (1) testing and updating the dimensionality of the IPC scale to enhance its relevance over time; (2) reevaluating the lower-order dimensions of IPC periodically, especially after significant social and technological changes that impact secondary usage or unauthorized monitoring of data as well as Internet users’ privacy perceptions; and (3) testing the conceptualization of the IPC model by Hong and Thong [44] with US-based data, since their model was based on data from respondents in Hong Kong. Thus, we validated the six dimensions proposed by Hong and Thong [44] and also extended their model by adding two additional dimensions, oversight and the RTBF. We provide theoretical and empirical evidence for our proposed integrated conceptualization. This research thus contributes to a better understanding of the conceptualization of IPC and provides a reliable and valid contemporary instrument for IPC.

5.3. Implications for Practice

This study suggests that in the post-Snowden era, oversight concerns cannot be ignored and will need to be modeled as part of IPC. This study has also demonstrated that the RTBF is a key component of IPC in the USA today, even if it is not a legal requirement for businesses to comply with. The research also has implications for individual users by raising awareness of *passive* privacy concerns, such as the RTBF, along with awareness versus *active* concerns – collection, secondary use, unauthorized usage, errors, control [44], and, as proposed in this study, oversight [46]. Our updated scale will help capture users' privacy concerns more realistically and completely. The revision of the IPC scale and the inclusion of oversight and RTBF concerns is very timely, as some US states, particularly California and Vermont among others, have enacted laws that go beyond breach notifications and require companies to make significant changes in their data processing operations. The California Consumer Privacy Act (CCPA), which came into force on January 1, 2020, has many similarities with Europe's General Data Protection Regulation (GDPR) rules, which legalized the RTBF. The CCPA and GDPR have a lot in common. Both laws deal with the same broad themes, such as transparency, and each lays down a similar right to delete personal information (RTBF) as well as a right to data portability [88]. A Vermont law, Act 171, that went into effect on January 1, 2019, aims at regulating data brokers [101]. Iowa enacted a law to protect students' information from being sold or rented [47]. Serrato et al. [82] provided information on some US states' recent privacy laws enacted on the heels of GDPR in Europe.

5.4. *Limitations and Future Research*

As with any research, it is important to acknowledge the limitations of our study. This study was carried out on the MTurk crowdsourcing platform, and hence, future research should test the model with a more diverse and representative sample of the US population as well as examine the model longitudinally. As noted earlier, IPC is a dynamic construct that will need to be examined over time to capture the essence of the construct to reflect its evolving multi-tiered structure – from single-factor, to second-order, to now third-order and beyond. Privacy concerns may continue to evolve as home security cameras, appliances, and health and fitness indicators become connected through the Internet of things to local businesses, medical providers, and other local and federal government agencies. It is also possible that the nature of the concern associated with the RTBF may change, and it may evolve from a less regarded privacy concern into one that is associated with an individual's right, and hence, from a passive concern into a more "direct" concern. We need more studies to validate and generalize the findings from this study [56]. Future research could use different types of information – varying in terms of context and sensitivity [12] – to examine the robustness of the proposed structure presented in this paper. Such examinations will also be helpful to settle the debate on whether the RTBF conflicts with the first US Constitutional amendment [53, 59, 90]. Moreover, it is generally recommended to have three or more items per factor, although the oversight, errors, and unauthorized access constructs in this study were measured with only two items each. However, it is noted that using two items is permitted if the items have fairly high convergent and discriminant validity [108].

5.5. *Conclusion*

This study extends the structure of the IPC scale by Hong and Thong [44] and provides empirical support to incorporate the RTBF and oversight concerns. The study provides and compares alternative models for IPC and discusses the merits of the proposed model. We measured and assessed the fit of a more enhanced and comprehensive set of IPC dimensions that includes oversight and the RTBF and verified that the proposed model fits well in the nomological network of IPC.

As users and citizens become more educated about how online businesses aid in government intrusion through unpublicized channels such as third-party doctrine [13], privacy concerns related to oversight due to surveillance will become even more salient. It is possible that future generations would be less worried about surveillance as they grow used to it [1] and as they weigh network externalities and benefits higher than privacy costs [45]. When that happens, we might need to revisit the scale again.

CRediT author statement

Gaurav Bansal: Conceptualization, Methodology, Software, Investigation, Data Curation, Writing - Original Draft, Visualization; **Fiona Fui-Hoon Nah**Conceptualization, Methodology, Validation, Writing - Reviewing and Editing.

Acknowledgments

The research was made possible in part due to Frederick E. Baer Professorship in Business at Austin E. Cofrin School of Business at the University of Wisconsin – Green Bay. We would also like to thank the editor-in-chief, the associate editor, and the reviewers for their constructive comments and suggestions that have helped enhance the paper.

APPENDIX A: Measurement Items

Table A1

Table A1
Measurement items

Answer the following questions on a scale of 1 (strongly disagree) to 7 (strongly agree)	
Please rate your level of concern when online companies…	
COL1	…ask you for your personal information.
COL2	…collect your personal information.
COL3	In general, I am concerned that online companies are collecting too much personal information on their users.
Please rate your level of concern when online companies...	
SEC1	…share your personal information with other companies without prior authorization.
SEC2	…sell your personal information with other companies.
SEC3	…misuse your personal information for other reasons without prior authorization.
With regard to preventing unauthorized access to personal information, please rate your level of concern that online companies may…	
UA1	…have poor procedures to prevent unauthorized access.
UA2	…devote insufficient time and effort to prevent unauthorized access.
With regard to correcting and verifying the accuracy of personal information, please rate your level of concern that online companies may...	
ERR1	…have poor controls over verifying the accuracy of personal information.
ERR2	…devote insufficient time and effort for verifying the accuracy of personal information.
AWA1	I am concerned when a clear and conspicuous disclosure is not included in the privacy policies of companies or government agencies.
AWA2	It usually bothers me when I am not aware or knowledgeable about how my personal information will be used by companies or government agencies.
AWA3	It usually bothers me when companies or government agencies do not tell me the way the data are collected, processed, and used.

(*continued on next page*)

Table A1 (*continued*)

RTBF1	I am concerned that companies or government agencies do not allow me to delete information I have given them.
RTBF2	It usually bothers me that companies or government agencies don't offer a process for me to request deletion of information I have given them.
RTBF3	I am concerned that companies or government agencies may not honor my requests to delete information I have given them.
CON1	It usually bothers me when I do not have control of personal information that I provide to companies or government agencies.
CON2	It usually bothers me when I do not have control or autonomy over decisions about how my personal information is collected, used, and shared by companies or government agencies.
CON3	I am concerned when control is lost or unwillingly reduced as a result of a marketing transaction with companies or government agencies.
OVE1	I am concerned that any information that I submit online could be used along with my other information to build an extensive profile on me.
OVE2	I am concerned that information that I submit online could be used to track my activities.
TRINT1	I believe that the Internet is now a robust and safe environment in which to transact.
TRINT2	I feel assured that legal structures adequately protect me from problems on the Internet.
TRINT3	I feel assured that technological structures adequately protect me from problems on the Internet.
TROB1	I feel that online businesses act in their customers' best interest.
TROB2	I am comfortable relying on online businesses to meet their obligations.
TGOV1	I feel that government acts in the citizens' best interest.
TGOV2	I feel fine interacting with the government since it generally fulfills its duties efficiently.
TGOV3	I always feel confident that I can rely on the government to do their part when I interact with them.
TRPR1	I feel that people are generally reliable.
TRPR2	I feel that people are generally honest.
TRPR3	I feel that people are generally dependable.

APPENDIX B: Computation of Alternate Models

We analyzed different IPC models by associating control with interaction management along with COL and SEC; and UA and ERR as information management as proposed and validated by Hong and Thong [44]. We associated RTBF, OVE, and AWA in different combinations as shown in Table B1 as validation for the support of our proposed model (Model 2).

In Table B2, we developed alternative models that freed CONTROL from interaction management by considering various possible combinations for CONTROL, RTBF, OVE, and AWA.

In Table B3, we provide the fit indices of the models developed in Tables B1 and B2. The models that were computed normally are highlighted. Out of 36 total model combinations examined, only six were computed normally; the rest could not be computed due to non-convergence caused by multicollinearity.

Table B4 shows the results of the fit indices along with R square from the estimation of the selected models from Table B3. Results show that Model 2 has superior fit indices and also demonstrates considerably high R square values for the trust constructs. Model 6 and 35 are close in terms of fit indices and R square values to Model 2. However, model 2 is supported by theoretical reasoning as discussed in the main paper.

Table B1
Construction of models

Model #	Information management (along with UA and ERR)	Interaction management (along with COL and SEC)	Third second-order factor	Fourth second-order factor	First-order factor
Model 1	First-order model comprising of all eight dimensions: UA, ERR, COL, SEC, OVE, CONTROL, RTBF, and AWA				
Model 2	-	CONTROL and OVE	-	-	AWA, RTBF
Model 3	RTBF	CONTROL and OVE	-	-	AWA
Model 4	-	CONTROL, OVE, and RTBF	-	-	AWA
Model 5	OVE, and RTBF	CONTROL	-	-	AWA
Model 6	-	CONTROL and RTBF	-	-	AWA, OVE
Model 7	-	CONTROL	-	-	AWA, OVE, RTBF
Model 8	-	CONTROL and RTBF	AWA and OVE	-	-
Model 9	-	CONTROL	AWA, OVE, and RTBF	-	-
Model 10	-	CONTROL	OVE and RTBF	-	AWA
Model 11	RTBF	CONTROL	AWA and OVE	-	-
Model 12	OVE	CONTROL and RTBF	-	-	AWA
Model 13	OVE	CONTROL	-	-	AWA, RTBF
Model 14	RTBF	CONTROL	-	-	AWA, OVE
Model 15	-	CONTROL	AWA and OVE	-	RTBF
Model 16	-	CONTROL	AWA AND RTBF	-	OVE

Table B2
Construction of other models.

Model #	Information management (along with UA and ERR)	Interaction management (along with COL and SEC)	Third second-order factor	Fourth second-order factor	First-order factor
Model 17	CONTROL	OVE and RTBF	-	-	AWA
Model 18	CONTROL, OVE, and RTBF	-	-	-	AWA
Model 19	CONTROL and RTBF	OVE	-	-	AWA
Model 20	CONTROL and OVE	RTBF	-	-	AWA
Model 21	-	OVE and RTBF	AWA and CONTROL	-	-
Model 22	CONTROL and RTBF	-	AWA and OVE	-	-
Model 23	CONTROL and RTBF	-	-	-	AWA, OVE
Model 24	-	-	-	CONTROL and RTBF	AWA, OVE
Model 25	-	-	AWA OVE	CONTROL RTBF	-
Model 26	-	-	CONTROL RTBF OVE	-	AWA
Model 27	-	-	CONTROL and OVE	-	AWA, RTBF
Model 28	RTBF	-	CONTROL and OVE	-	AWA
Model 29	-	RTBF	CONTROL and OVE	-	AWA
Model 30	OVE	-	CONTROL and RTBF	-	AWA
Model 31	-	OVE	CONTROL and RTBF	-	AWA
Model 32	-	-	AWA OVE	CONTROL RTBF	-
Model 33	CONTROL	OVE	-	-	AWA, RTBF
Model 34	RTBF OVE	-	-	-	AWA, CONTROL
Model 35	-		-	-	AWA RTBF OVE CONTROL
Model 36	-	OVE and RTBF	-	-	AWA CONTROL

Measurement models

Fit indices	Chi sq/df	CFI	TLI	RMSEA	SRMR	Remarks
Model 1 CFA	777.137/477	.924	.915	.049	.059	Computed normally
Model 2 CFA	756.357/475	.928	.920	.048	.060	Computed normally
Model 3 CFA	774.918/475	.924	.915	.049	.054	PC1 is undefined*. High correlation between PC and PC1.
Model 4 CFA	749.534/475	.930	.922	.047	.060	AWA and CON are undefined*. High correlation between PC and AWA; and PC2 and CON.
Model 5 CFA	780.210/475	.922	.914	.050	.062	PC2 is undefined*. High correlation between PC and PC2.
Model 6 CFA	754.000/475	.929	.921	.047	.059	Computed normally
Model 7 CFA	754.389/475	.929	.921	.047	.058	PC2 is undefined*. High correlation between PC and control, and also between PC and PC2.
Model 8 CFA	751.526/474	.929	.921	.047	.063	PC3 is undefined*. High correlation between PC and AWA; PC3 and CON; and PC2 and PC3.
Model 9 CFA	748.827/474	.930	.922	047.	.053	PC3 is undefined*. High correlation between PC3 and CON; PC3 and PC2; and PC and PC3.
Model 10 CFA	751.610/474	.929	.921	.047	.054	PC2 is undefined*. High correlation between PC and PC2.
Model 11 CFA	777.373/474	.923	.914	.049	.061	PC2 and PC3 are undefined*. High correlation between PC3 and CON; PC2 and PC1; PC1 and PC3; PC2 and PC3; PC2 and PC; and PC3 and PC.
Model 12 CFA	767.032/475	.926	.917	.048	.057	Computed normally
Model 13 CFA	771.942/475	.924	.916	.049	.061	PC2 is undefined*. High correlation between PC2 and PC high corr.
Model 14 CFA	777.304/475	.923	.915	.049	.058	PC2 is undefined*. High correlation between PC1 and PC2; and PC2 and PC.
Model 15 CFA	752.702/474	.929	.921	.047	.058	PC2 and PC3 are undefined*. High correlation between PC3 and CON; PC2 and PC3; PC2 and PC; and PC3 and PC.
Model 16 CFA	754.902/474	.929	.920	.048	.058	PC2 and PC3 are undefined*. High correlation between PC3 and CON; PC2 and PC3; PC2 and PC; and PC3 and PC.
Model 17 CFA	771.381/475	.925	.916	.049	.061	PC1 is undefined*. High correlation between PC1 and AWA; and, PC and CON.
Model 18 CFA	777.692/475	.923	.914	.049	.060	PC1 is undefined*. High correlation between PC and PC1.
Model 19 CFA	778.342/475	.923	.914	.049	.062	PC1 is undefined*. High correlation between PC and PC1; and PC and CON.
Model 20 CFA	775.271/475	.924	.915	.049	.061	PC1 and PC2 are undefined*. High correlation between PC and CON; PC2 and CON; PC and PC1; PC and PC2; and PC1 and PC2.
Model 21 CFA	757.761/474	.928	.920	.048	.064	CON and PC2 are undefined*. High correlation between PC2 and CON; PC3 and CON; and PC2 and PC.
Model 22 CFA	776.540/474	.923	.914	.049	.062	PC1 and PC3 are undefined*. High correlation between PC3 and CON; PC3 and PC1; PC and PC1; PC2 and PC3; and PC and PC3.
Model 23 CFA	778.227/475	.923	.914	.049	.062	PC1 is undefined*. High correlation between PC and CON; PC and PC1.
Model 24 CFA	750.558/474	.930	.922	.047	.061	CON is undefined*. High correlation between PC4 and CON.
Model 25 CFA	746.729/473	.930	.922	.047	.061	CON and PC3 are undefined*. High correlation between PC3 and CON; PC4 and CON; PC2 and PC3; PC3 and PC4; and PC3 and PC.
Model 26 CFA	746.084/474	.931	.923	.047	.060	CON is undefined*. High correlation between PC3 and CON.
Model 27 CFA	756.416/474	.928	.920	.048	.062	CON is undefined*. High correlation between PC3 and CON.
Model 28 CFA	778.390/474	.923	.914	.050	.061	CON and PC1 are undefined*. High correlation between PC3 and CON; and PC and PC1.
Model 29 CFA	754.870/474	.929	.920	.048	.059	CON and PC2 are undefined*. High correlation between PC2 and CON; PC3 and CON; and PC and PC2.
Model 30 CFA	764.250/474	.926	.918	.048	.060	Con is undefined*. High correlation between PC3 and CON.
Model 31 CFA	749.142/474	.930	.922	.047	.057	CON is undefined*. High correlation between PC3 and CON.
Model 32 CFA	746.729/473	.930	.922	.047	.061	CON and PC3 are undefined*. High correlation between PC3 and CON; PC4 and CON; PC2 and PC4; PC2 and PC3; PC3 and PC4; and PC3 and PC.
Model 33 CFA	768.830/475	.925	.917	.049	.056	PC1 is undefined*. High correlation between PC1 and AWA; and PC and CON.
Model 34 CFA	777.891/475	.923	.914	.049	.061	Computed normally
Model 35 CFA	755.754/475	.929	.921	.047	.062	Computed normally
Model 36 CFA	753.249/475	.929	.921	.047	.055	PC2 is undefined*. High correlation between PC2 and PC.

Note: * residual variance is undefined: residual variance is negative and hence it could not be computed by Mplus (999 is printed when a value cannot be computed). A negative residual variance is caused by correlation > 1 that makes the results inadmissible (source: http://www.statmodel.com/discussion/messages/8/5487.html?1485893543); PC1 refers to information management; PC2 refers to interaction management; PC refers to overall Internet privacy concern

Table B4
Fit indices for the estimation models

Fit indices	Model 1 (base)	Model 2	Model 6	Model 12	Model 34	Model 35
Chi sq / df	777.156/477	754.071/475	755.231/475	770.560/475	780.624/475	754.955/475
CFI	.924	.929	.929	.925	.922	.929
TLI	.915	.921	.921	.916	.914	.921
RMSEA	.049	.047	.047	.049	.050	.047
SRMR	.056	.055	.055	.058	.057	.055
Rsq TRINT	.441	.458	.436	.459	.439	.439
Rsq TROB	.338	.352	.334	.354	.336	.334
Rsq TGOV	.533	.544	.530	.544	.531	.537

APPENDIX C: Factor Loadings

Table C1

Table C1
Factor loadings for lower-level constructs in Model 2 (estimation model)

Construct	Item	Factor Loading	T-Stat
COL	COL1	0.774	19.820
	COL2	0.811	22.476
	COL3	0.744	15.121
SEC	SEC1	0.841	26.510
	SEC2	0.792	17.924
	SEC3	0.775	14.928
UA	UA1	0.824	24.981
	UA2	0.847	25.371
ERR	ERR1	0.774	17.083
	ERR2	0.807	20.647
AWA	AWA1	0.737	18.685
	AWA2	0.748	19.822
	AWA3	0.770	22.017
RTBF	RTBF1	0.854	33.380
	RTBF2	0.737	16.403
	RTBF3	0.812	30.365
CON	CON1	0.764	22.734
	CON2	0.766	20.869
	CON3	0.713	14.637
OVE	OVE1	0.777	17.695
	OVE2	0.755	15.863
TRINT	TRINT1	0.795	21.328
	TRINT2	0.804	27.241
	TRINT3	0.809	26.203
TROB	TROB1	0.835	26.380
	TROB2	0.768	19.446
	TROB3	0.780	19.421
TGOV	TGOV1	0.879	37.895
	TGOV2	0.823	20.784
	TGOV3	0.865	38.273
TRPR	TRPR1	0.820	24.313
	TRPR2	0.829	24.054
	TRPR3	0.837	25.960

References

[1] A. Acquisti, L. Brandimarte, G. Loewenstein, Privacy and human behavior in the age of information, Science 347 (6221) (2015) 509–514.

[2] P.E. Agre, Surveillance and capture: Two models of privacy, The Information Society 10 (2) (1994) 101–127.

[3] AICPA/CICA, Records Management: Integrating Privacy Using Generally Accepted Privacy Principles [https://www.aicpa.org/content/dam/aicpa/interestareas/informationtechnology/resources/privacy/downloadabledocuments/10252-346-records-management-pro.pdf (last accessed July 27, 2021)], 2009.

[4] C.M. Angst, Protect my privacy or support the common-good? Ethical questions about electronic health information exchanges, Journal of Business Ethics 90 (2) (2009) 169–178.

[5] S.S. Ariss, Computer monitoring: benefits and pitfalls facing management, Information & Management 39 (7) (2002) 553–558.

[6] Association for Computing Machinery, Code of Ethics, Communications of the ACM 23 (7) (1980), 425-425.

[7] B. Auxier, Most Americans support right to have some personal info removed from online searches [https://www.pewresearch.org/fact-tank/2020/01/27/most-americans-support-right-to-have-some-personal-info-removed-from-online-searches/ (last accessed Aug 14, 2020)], 2020.

[8] B. Auxier, L. Rainie, M. Anderson, A. Perrin, M. Kumar, E. Turner, Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information [https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/ (last accessed Jan 28, 2020)], 2019.

[9] N.F. Awad, M.D. Krishnan, The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization, MIS Quarterly 30 (1) (2006) 13–28.

[10] R.P. Bagozzi, An Examination of the Validity of Two Models of Attitude, Multivariate Behavioral Research 16 (3) (1981) 323–359.

[11] G. Bansal, F. Zahedi, D. Gefen, The role of privacy assurance mechanisms in building trust and the moderating role of privacy concern, European Journal of Information Systems 24 (6) (2015) 624–644.

[12] G. Bansal, F.M. Zahedi, D. Gefen, Do context and personality matter? Trust and privacy concerns in disclosing private information online, Information & Management 53 (1) (2016) 1–21.

[13] M. Bedi, Facebook and interpersonal privacy: Why the third party doctrine should not apply, Boston College Law Review 54 (2013) 1–71.

[14] F. Bélanger, L. Carter, Trust and risk in e-government adoption, Journal of Strategic Information Systems 17 (2) (2008) 165–176.

[15] F. Bélanger, R.E. Crossler, Privacy in the digital age: A review of information privacy research in information systems, MIS Quarterly 35 (4) (2011) 1017–1041.

[16] R.W. Bellaby, Going dark: anonymising technology in cyberspace, Ethics and Information Technology 20 (3) (2018) 189–204.

[17] S.C. Bennett, The right to be forgotten: Reconciling EU and US perspectives, Berkeley Journal of International Law 30 (2012) 161–195.

[18] C. Bloom, J. Tan, J. Ramjohn, L. Bauer, Self-driving cars and data collection: Privacy perceptions of networked autonomous vehicles, in: the Proceedings of *Thirteenth Symposium on Usable Privacy and Security*, 2017.

[19] C. Botan, Communication work and electronic surveillance: A model for predicting panoptic effects, Communications Monographs 63 (4) (1996) 293–313.

[20] L.A. Bygrave, A right to be forgotten? Communications of the ACM 58 (1) (2014) 35–37.

[21] J.E. Campbell, M. Carlson, Panopticon.com: Online surveillance and the commodification of privacy, Journal of Broadcasting & Electronic Media 46 (4) (2002) 586–606.

[22] J.T. Child, J.C. Pearson, S. Petronio, Blogging, communication, and privacy management: Development of the blogging privacy management measure, Journal of the American Society for Information Science and Technology 60 (10) (2009) 2079–2094.

[23] S. Conger, J.H. Pratt, K.D. Loch, Personal information privacy and emerging technologies, Information Systems Journal 23 (2012) 1–17.

[24] J. Correia, D. Compeau, Information privacy awareness (IPA): a review of the use, definition and measurement of IPA, in: the Proceedings of *Proceedings of the 50th Hawaii International Conference on System Sciences*, 2017.

[25] R.E. Crossler, C. Posey, Robbing Peter to Pay Paul: Surrendering Privacy for Security's Sake in an Identity Ecosystem, Journal of the Association for Information Systems 18 (7) (2017) 487–515.

[26] M.J. Culnan, How did they get my name: An exploratory investigation of customer attitudes toward secondary information use, MIS Quarterly 17 (3) (1993) 341–361.

[27] M.J. Culnan, R.J. Bies, Consumer privacy: Balancing economic and justice considerations, Journal of Social Issues 59 (2) (2003) 323–342.

[28] M.J. Culnan, C.C. Williams, How ethics can enhance organizational privacy: Lessons from the Choicepoint and TJX data breaches, MIS Quarterly 33 (4) (2009) 673–687.

[29] S.C. D'Urso, Who's watching us at work? Toward a structural–perceptual model of electronic monitoring and surveillance in organizations, Communication Theory 16 (3) (2006) 281–303.

[30] T. Dinev, M. Bellotto, P. Hart, V. Russo, I. Serra, Internet users' privacy concerns and beliefs about government surveillance: An exploratory study of differences between Italy and the United States, Journal of Global Information Management 14 (4) (2006) 57–93.

[31] T. Dinev, P. Hart, Internet privacy concerns and their antecedents-measurement validity and a regression model, Behaviour & Information Technology 23 (6) (2004) 413–422.

[32] T. Dinev, P. Hart, An extended privacy calculus model for e-commerce transaction, Information Systems Research 17 (1) (2006) 61–80.

[33] T. Dinev, P. Hart, M.R. Mullen, Internet privacy concerns and beliefs about government surveillance–An empirical investigation, The Journal of Strategic Information Systems 17 (3) (2008) 214–233.

[34] J.B. Earp, A.I. Antón, L. Aiman-Smith, W.H. Stufflebeam, Examining Internet privacy policies within the context of user privacy values, IEEE Transactions on Engineering Management 52 (2) (2005) 227–237.

[35] D.H. Flaherty, Controlling Surveillance: Can Privacy Protection Be Made Effective? in: P.E.A.a.M. Rotenberg (Ed.), ***Technology and Privacy: The New Landscape*** MIT Press, 1997, pp. 167–192.

[36] B.A. Friedman, L.J. Reed, Workplace privacy: Employee relations and legal implications of monitoring employee e-mail use, Employee Responsibilities and Rights Journal 19 (2) (2007) 75–83.

[37] H. Galanxhi, F.F.-H. Nah, Privacy issues in the era of ubiquitous commerce, Electronic Markets 16 (3) (2006) 222–232.

[38] G. Gao, What Americans think about NSA surveillance, national security and privacy [https://www.pewresearch.org/fact-tank/2015/05/29/what-americans-think-about-nsa-surveillance-national-security-and-privacy/ (last accessed Jan 28 2020)], 2015.

[39] A.W. Geiger, How Americans have viewed government surveillance and privacy since Snowden leaks [https://www.pewresearch.org/fact-tank/2018/06/04/how-americans-have-viewed-government-surveillance-and-privacy-since-snowden-leaks/ (last accessed Feb 28, 2020)], 2018.

[40] HLR, Cooperation or Resistance?: The Role of Tech Companies in Government Surveillance [https://harvardlawreview.org/2018/04/cooperation-or-resistance-the-role-of-tech-companies-in-government-surveillance/ (last accessed Mar 5, 2020)], 2018.

[41] H. Hoehle, J.A. Aloysius, S. Goodarzi, V. Venkatesh, A nomological network of customers' privacy perceptions: linking artifact design to shopping efficiency, European Journal of Information Systems 28 (1) (2019) 91–113.

[42] A. Holzinger, S. Dorner, M. Födinger, A.C. Valdez, M. Ziefle, Chances of increasing youth health awareness through mobile wellness applications, in: the Proceedings of *Symposium of the Austrian HCI and Usability Engineering Group*, 2010.

[43] A. Holzinger, K. Schaupp, W. Eder-Halbedl, An investigation on acceptance of ubiquitous devices for the elderly in a geriatric hospital environment: using the example of person tracking, in: the Proceedings of *International Conference on Computers for Handicapped Persons*, 2008.

[44] W. Hong, J.Y. Thong, Internet privacy concerns: An integrated conceptualization and four empirical studies, MIS Quarterly 37 (1) (2013) 275–298.

[45] C.-L. Hsu, J.C.-C. Lin, An empirical examination of consumer adoption of Internet of Things services: Network externalities and concern for information privacy perspectives, Computers in Human Behavior 62 (2016) 516–527.

[46] Human Rights Watch, US: New Evidence Suggests Monitoring of Americans - Documents Point to Warrantless Surveillance [https://www.hrw.org/news/2017/10/25/us-new-evidence-suggests-monitoring-americans (last accessed Sep 6, 2020)], 2017.

[47] Iowa.gov, An act relating to student personal information protection [https://www.legis.iowa.gov/legislation/BillBook?ga=87&ba=HF2354 (last accessed Sep 6, 2020)], 2018.

[48] T.L. James, M. Warkentin, S.E. Collignon, A dual privacy decision model for online social networks, Information & Management 52 (8) (2015) 893–908.

[49] E.E. Joh, Privacy protests: surveillance evasion and fourth amendment suspicion, Ariz. L. Rev. 55 (2013) 997–1029.

[50] M.-C. Kim, Surveillance technology, privacy and social control: with reference to the case of the electronic national identification card in South Korea, International sociology 19 (2) (2004) 193–213.

[51] S. Kurkovsky, E. Syta, Monitoring of electronic communications at universities: Policies and perceptions of privacy, in: the Proceedings of *2011 44th Hawaii International Conference on System Sciences*, 2011.

[52] C. Kwak, J. Lee, K. Park, H. Lee, Let Machines Unlearn–Machine Unlearning and the Right to be Forgotten, in: the Proceedings of *Americas Conference on Information Systems*, 2017.

[53] R.G. Larson III, Forgetting the First Amendment: How obscurity-based privacy and a right to be forgotten are incompatible with free speech, Communication Law and Policy 18 (1) (2013) 91–120.

[54] R.S. Laufer, M. Wolfe, Privacy as a concept and a social issue: A multidimensional development theory, Journal of Social Issues 33 (3) (1977) 22–42.

[55] M.K. Lindell, D.J. Whitney, Accounting for Common Method Variance in Cross-Sectional Research Designs, Journal of Applied Psychology 86 (1) (2001) 114–121.

[56] S.B. MacKenzie, P.M. Podsakoff, N.P. Podsakoff, Construct measurement and validation procedures in MIS and behavioral research: Integrating new and existing techniques, MIS Quarterly 35 (2) (2011) 293–334.

[57] N.K. Malhotra, S.S. Kim, J. Agarwal, Internet users' Internet information privacy concerns (IUIPC): The construct, the scale, and a causal model, Information Systems Research 15 (4) (2004) 336–355.

[58] S. Mamonov, M. Koufaris, The impact of exposure to news about electronic government surveillance on concerns about government intrusion, privacy self-efficacy, and privacy protective behavior, Journal of Information Privacy and Security 12 (2) (2016) 56–67.

[59] A. Mantelero, The EU Proposal for a General Data Protection Regulation and the roots of the 'right to be forgotten, Computer Law & Security Review 29 (3) (2013) 229–235.

[60] A. Marthews, C.E. Tucker, Government surveillance and internet search behavior, SSRN 2412564 (2017) 1–53.

[61] K.E. Martin, Ethical issues in the big data industry, MIS Quarterly Executive 14 (2) (2015) 67–85.

[62] N. Martin, The Major Concerns Around Facial Recognition Technology [https://www.forbes.com/sites/nicolemartin1/2019/09/25/the-major-concerns-around-facial-recognition-technology/#6a3682174fe3 (last accessed Sep 4, 2020)], 2019.

[63] R.O. Mason, Four ethical issues of the information age, MIS Quarterly 10 (1) (1986) 5–12.

[64] A. Miller, ***Computers and Privacy in Ethics and the Management of Computer Technology*** (W. M. Hoffman, a. J. M. M., ed), Oelgeschlager, Gunn, and Hain Publishers, Inc., Cambridge, MA, 1982.

[65] G.R. Milne, A.J. Rohm, Consumer privacy and name removal across direct marketing channels: Exploring opt-in and opt-out alternatives, Journal of Public Policy & Marketing 19 (2) (2000) 238–249.

[66] C.L. Miltgen, H.J. Smith, Exploring information privacy regulation, risks, trust, and behavior, Information & Management 52 (6) (2015) 741–759.

[67] V. Mitsilegas, The transformation of privacy in an era of pre-emptive surveillance, Tilburg Law Review 20 (1) (2015) 35–57.

[68] L.K. Muthén, B.O. Muthén, ***Mplus User's Guide*** (Seventh Edition). Los Angeles, CA: Muthén & Muthén, 1998-2012.

[69] A. Newcomb, A timeline of Facebook's privacy issues — and its responses [https://www.nbcnews.com/tech/social-media/timeline-facebook-s-privacy-issues-its-responses-n859651 (last accessed Sep 4, 2020)], 2018.

[70] A.L. Newman, What the "right to be forgotten" means for privacy in a digital age, Science 347 (6221) (2015) 507–508.

[71] K. O'Hara, The right to be forgotten: the good, the bad, and the ugly, IEEE Internet Computing 19 (4) (2015) 73–79.

[72] S. O'Sullivan, N. Nevejans, C. Allen, A. Blyth, S. Leonard, U. Pagallo, K. Holzinger, A. Holzinger, M.I. Sajid, H. Ashrafian, Legal, regulatory, and ethical frameworks for development of standards in artificial intelligence (AI) and autonomous robotic surgery, The International Journal of Medical Robotics and Computer Assisted Surgery 15 (e1968) (2019) 1–12.

[73] A. Oulasvirta, T. Suomalainen, J. Hamari, A. Lampinen, K. Karvonen, Transparency of intentions decreases privacy concerns in ubiquitous surveillance, Cyberpsychology, Behavior, and Social Networking 17 (10) (2014) 633–638.

[74] S. Petronio, Communication privacy management theory: What do we know about family privacy regulation? The Journal of Family Theory & Review 2 (3) (2010) 175–196.

[75] PriceWaterHouse Coopers, Consumer Intelligence Series: Prepare for the voice revolution [https://www.pwc.com/us/en/advisory-services/publications/consumer-intelligence-series/voice-assistants.pdf (last accessed Sep 4, 2020)], 2018.

[76] L. Rainie, Americans' complicated feelings about social media in an era of privacy concerns [https://www.pewresearch.org/fact-tank/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy-concerns (last accessed Mar 12, 2020)], 2018.

[77] L. Rainie, M. Madden, How People are Changing Their Own Behavior [https://www.pewresearch.org/internet/2015/03/16/how-people-are-changing-their-own-behavior/ (last accessed April 22, 2020)], 2015.

[78] L. Rainie, A. Perrin, Key findings about Americans' declining trust in government and each other [https://www.pewresearch.org/fact-tank/2019/07/22/key-findings-about-americans-declining-trust-in-government-and-each-other/ (last accessed Feb 10, 2020)], 2019.

[79] C.G. Reddick, A.T. Chatfield, P.A. Jaramillo, Public opinion on National Security Agency surveillance programs: A multi-method approach, Government Information Quarterly 32 (2) (2015) 129–141.

[80] P.M. Regan, J. Jesse, Ethical challenges of edtech, big data and personalized learning: twenty-first century student sorting and tracking, Ethics and Information Technology 21 (3) (2019) 167–179.

[81] J.P. Semitsu, From Facebook to mug shot: How the dearth of social networking privacy rights revolutionized online government surveillance, Pace L. Rev. 31 (2011) 291.

[82] J.K. Serrato, C. Cwalina, A. Rudawski, T. Coughlin, K. Fardelmann, US states pass data protection laws on the heels of the GDPR [https://www.dataprotectionreport.com/2018/07/u-s-states-pass-data-protection-laws-on-the-heels-of-the-gdpr/], 2018.

[83] S. Sharma, R.E. Crossler, Disclosing too much? Situational factors affecting information disclosure in social commerce environment, Electronic Commerce Research and Applications 13 (5) (2014) 305–319.

[84] K.B. Sheehan, M.G. Hoy, Dimensions of privacy concern among online consumers, Journal of Public Policy & Marketing 19 (1) (2000) 62–73.

[85] H.J. Smith, T. Dinev, H. Xu, Information privacy research: An interdisciplinary review, MIS Quarterly 35 (4) (2011) 992–1015.

[86] H.J. Smith, S.J. Milberg, S.J. Burke, Information privacy: Measuring individuals' concerns about organizational practices, MIS Quarterly 20 (2) (1996) 167–196.

[87] D.J. Solove, A taxonomy of privacy, University of Pennsylvania Law Review 154 (2005) 477–560.

[88] G. Somers, L. Boghaert, The California Consumer Privacy Act and the GDPR: two of a kind? [https://www.financierworldwide.com/the-california-consumer-privacy-act-and-the-gdpr-two-of-a-kind (last accessed Sep 6, 2020)], 2018.

[89] P. Steinbart, M. Keith, J. Babb, The Right to be Forgotten: Exploring Consumer Privacy Attitudes About the Final Stage of the Information Life Cycle, in: the Proceedings of *2015 Dewald Roode Workshop on Information Systems Security Research, IFIP WG8.11/WG11* 13, 2015.

[90] P. Steinbart, M. Keith, J. Babb, Measuring Privacy Concern and the Right to Be Forgotten, in: the Proceedings of *50th Hawai'i International Conference on System Sciences*, 2017.

[91] P.J. Steinbart, D. Truog, M.J. Keith, J. Babb, The Right to Be Forgotten: Exploring Consumer Privacy Attitudes About the Final Stage of the Information Life Cycle, Available at SSRN 2563333, 2015, pp. 1-38.

[92] K.A. Stewart, A.H. Segars, An empirical examination of the concern for information privacy instrument, Information Systems Research 13 (1) (2002) 36–49.

[93] E.F. Stone-Romero, D.L. Stone, D. Hyatt, Personnel selection procedures and invasion of privacy, Journal of Social Issues 59 (2) (2003) 343–368.

[94] E.F. Stone, H.G. Gueutal, D.G. Gardner, S. McClure, A field experiment comparing information-privacy values, beliefs, and attitudes across several types of organizations, Journal of Applied Psychology 68 (3) (1983) 459–468.

[95] E. Stoycheff, Under surveillance: Examining Facebook's spiral of silence effects in the wake of NSA internet monitoring, Journalism & Mass Communication Quarterly 93 (2) (2016) 296–311.

[96] T.S. Teo, S.C. Srivastava, L. Jiang, Trust and electronic government success: An empirical study, Journal of Management Information Systems 25 (3) (2008) 99–132.

[97] N. Thompson, T. McGill, A. Bunn, R. Alexander, Cultural factors and the role of privacy concerns in acceptance of government surveillance, Journal of the Association for Information Science and Technology 71 (9) (2020) 1129–1142.

[98] R. Turn, ***Privacy protection in information systems in Advances in Computers***, Elsevier, 1977, pp. 221–335.

[99] R. Turn, W.H. Ware, Privacy and security issues in information systems in *Ethical issues in the use of computers*, 1985, 133-147.

[100] J. Verble, NSA The, Edward Snowden, surveillance in the 21st century, ACM SIGCAS Computers and Society 44 (3) (2014) 14–20.

[101] Vermont.Gov, H.764 (Act 171) An act relating to data brokers and consumer protection [https://legislature.vermont.gov/bill/status/2018/H.764 (last accessed Sep 6, 2020)], 2018.

[102] E.F. Villaronga, P. Kieseberg, T. Li, Humans forget, machines remember: Artificial intelligence and the right to be forgotten, Computer Law & Security Review 34 (2) (2018) 304–313.

[103] S.M. West, Data capitalism: Redefining the logics of surveillance and privacy, Business & society 58 (1) (2019) 20–41.

[104] Wired.com, Big Business Becoming Big Brother [https://www.wired.com/2004/08/big-business-becoming-big-brother/ (last accessed Sep 4, 2020)], 2004.

[105] World Health Organization, Surveillance [http://www.who.int/tobacco/surveillance/about_surveillance/en/index.html (last accessed July 25, 2021)], 2012.

[106] H. Xu, S. Gupta, M.B. Rosson, J.M. Carroll, Measuring mobile users' concerns for information privacy, in: the Proceedings of *Thirty Third International Conference on Information Systems*, Orlando, 2012.

[107] H.-L. Yang, R.-X. Lin, The impacts of SOLOMO services technostress on anxiety, Journal of Electronic Commerce Research 19 (2) (2018) 186–200.

[108] A.G. Yong, S. Pearce, A beginner's guide to factor analysis: Focusing on exploratory factor analysis, Tutorials in quantitative methods for psychology 9 (2) (2013) 79–94.

[109] D. Zweig, J. Webster, Where is the line between benign and invasive? An examination of psychological barriers to the acceptance of awareness monitoring systems, Journal of Organizational Behavior 23 (5) (2002) 605–633.

Dr. Gaurav Bansal is Frederick E. Baer Professor in Business and full professor of MIS/Statistics at the Austin E. Cofrin School of Business at University of Wisconsin-Green Bay. He is a Distinguished Member (Cum Laude) of the Association for Information Systems (AIS). He currently serves as editor-in-chief for the Journal of Information Technology Case and Application Research. He earned his Ph.D. in Management Information Systems from the University of Wisconsin – Milwaukee in 2008. He has published in several premier MIS journals such as Journal of Management Information Systems, European Journal of Information Systems, Decision Support Systems, and Information & Management. He has served as the past president of the Midwest Association for Information Systems.

Dr. Fiona Fui-Hoon Nah is a Professor at the City University of Hong Kong. She is a Distinguished Member of the Association for Information Systems (AIS). She currently serves as editor-in-chief of the AIS Transactions on Human–Computer Interaction. She received her Ph.D. in Management Information Systems from the University of British Columbia. Her publications have appeared in journals such as MIS Quarterly, Journal of the Association for Information Systems, Journal of Strategic Information Systems, Journal of Information Technology, International Journal of Human-Computer Studies, International Journal of Human–Computer Interaction, and Computers in Human Behavior. She is a co-founder and former chair of the AIS Special Interest Group on Human–Computer Interaction.